Insight on Internet Banking Crimes & Prevention

Kumaran K

Agenda :

i. A. Background of Internet banking
ii. B. Internet Usage in India
iii. C. Types of Online & Mobile frauds in India
iv. D. Cybercrime Prevention Safety tips

Background

Internet Banking started in the late 1990s. ICICI was the first bank to champion its usage and introduced Internet Banking to their customers in 1996. Banks like HDFC, Citibank and IndusInd followed. SBI launched Internet Banking in 2001. Anywhere Banking got recognized and services like checking account status, fund transfers, ordering demand drafts, loan applications and shopping portals were viewed as high value offerings. Total transaction value in the Digital Payments segment amounts to US$64,787m in 2019 from about 513.8m users in India. The market's largest segment is Digital Commerce with a total transaction value of US$58,812m in 2019. Total transaction value is expected to show an annual growth rate (CAGR 2019-2023) of 20.1% resulting in the total amount of US$134,588m by 2023. A total of 5,743 fraud incidents involving a total amount of Rs. 95,760 crores from Apr 2019 to Sep 2019 reported from Public Sector Banks. (Source – Business Standard, Nov 20,2019)

B. Internet Usage in India

This statistic provides information on the number of internet users in India from 2015 to 2023. In 2018, India had 483 million internet users. This figure is projected to grow to 666.4 million internet users in 2023. Despite the untapped potential, India already is the second-largest online market worldwide. The majority of India's internet users are mobile phone internet users, who take advantage of cheap alternatives to expensive landline connections that require desktop PCs and infrastructure. As of 2016, India had 320.57 million mobile phone internet users and forecasts estimate 492.68 million Indian mobile phone internet users by 2022. (Source - https://www.statista.com)

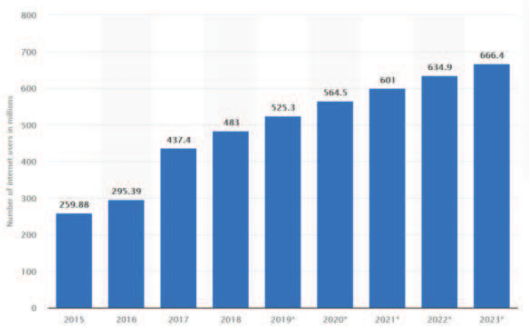


Fig. 1. Number of internet users in India from 2015 to 2023 (in millions)

C. Types of Online and Mobile Banking Frauds in India

C.1. Phishing

Process of collecting personal information through emails or websites claiming to be legitimate.

C.2. Spoofing

Is a fraudulent or malicious practice communication sent from unknown source disguised as a source known to the receiver.

C.3. Card Skimming

Theft of credit and debit card data and PIN numbers when the user is at an automated teller machine (ATM) or point of sale (POS). Card skimming allows thieves to steal money from accounts, make purchases and sell card information to third parties for the same purposes.

C.4. Page Jacking

Process of illegally copying legitimate website content to another website designed to replicate the original website and divert traffic from original site to cloned Web pages.

C.5. Juice Jacking

Juice jacking is a type of cyber-attack involving a charging port that doubles as a data connection, typically over USB. This often involves either installing malware or surreptitiously copying sensitive data from a smart phone, tablet, or other computer device.

C.6. QR Code Scam

A QR code is like a bar code, an image that can be read by a machine. It allows people to make payments by scanning the image and confirming the transaction. Many apps and e-wallets have this feature for easy payment. Most cases QR codes contained malware that drain information from smartphones.

C.7. SIM Swap Fraud

A SIM swap scam (also known as port-out scam, SIM splitting, and SIM jacking, SIM swapping) is a type of account takeover fraud that generally targets a weakness in two-factor authentication and two-step verification in which the second factor or step is a text message (SMS) or call placed to a mobile telephone. Fraudster contacts the victim's mobile operator and claiming that he has lost the phone. He reaches to the victim to press 1 to approve the SIM swap. Post this the fraudster will start receiving all SMS, OTPs, phone calls and so on.

C.8. Denial of Service

A denial-of-service (DoS) attack is a type of cyber-attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to addition users. A DoS attack is characterized by using a single computer to launch the attack. A distributed denial-of-service (DDoS) attack is a type of DoS attack that comes from many distributed sources, such as a botnet DDoS attack.

C.9. Buffer Overflow Attacks

An attack type in which a memory buffer overflow can cause a machine to consume all available hard disk space, memory, or CPU time. This form of exploit often results in sluggish behavior, system crashes, or other deleterious server behaviors, resulting in denial-of-service.

C.10. Flood Attacks

By saturating a targeted server with an overwhelming amount of packets, a malicious actor is able to oversaturate server capacity, resulting in denial-of-service. In order for most DoS flood attacks to be successful, the malicious actor must have more available bandwidth than the target.

C.11. Malware

Malware is a software that takes control of any individual computer to spread a bug to other people's devices or social networking profiles. These software can be used to create a botnet, a network of computers controlled remotely by Hackers to spread spam and viruses. Malvertising is using advertising to infect people and business.

C.12. Ransomware

Ransomware is a type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. Advanced malware uses a technique called crypto-viral extortion in which encrypts the victim's file and demands ransom to decrypt them. Ukash, Bitcoin and Altcoins (ex. Ethereum and NEO) are types of Cryptocurrency.

C.13. Scareware

Using fear tactics, cyber criminals compel users to download certain software. Some are projected as Antivirus software while others could be some other mobile applications. Once installed, these programs start attacking the user's system. User is then forced to pay the criminals to remove such viruses.

D. Safety Tips

D.1. Bank Related

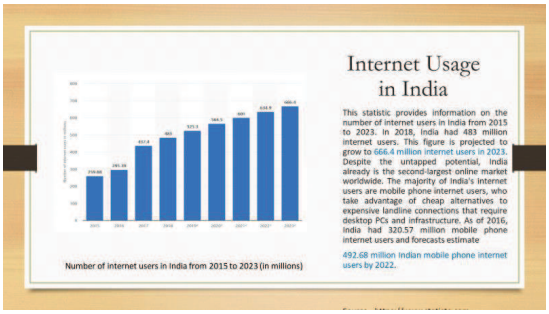
Avoid hacker calls or emails – No bank will call you and ask for your Bank Account details or any information regarding fund transfer. Keep Net Banking PIN and Password secret. Ideally plan a passphrase which you could remember easily. Do not share your account number to other people especially when you are in a bank. Avoid requesting strangers to fill up forms. Change password frequently. Do not use public computers for Online Banking. Especially avoid bank transactions while working in a cyber-café. Do not click on any link embedded in email/text message without verifying the authentication. Report any lost card immediately. Call the bank immediately and block the card. If you sense any transactions done already, also file a cyber crime complaint. Do not write or store your Key details in paper/system/calendars/phone. Try not to share your credit/debit to any unknown persons for any purposes. Do not share your OTP SMS & email alerts from your mobile. If your mobile has stopped working for unusual reasons, check with your mobile operator immediately. Register for SMS and email alerts to stay informed on your bank account to avoid SIM swap related frauds. Do not fill up online forms for letting your space for ATMs/Cell Towers. If you wish to rent do a physical check with the nearby Banks or Service providers. Set up daily withdrawal limit, say Rs.5000 or less. This will prevent the hijacker to withdraw bulk amounts. Wait till the screen refreshes to a new screen after you complete all transactions in the ATM post sign out. Do not click "I Accept" button while logging out in ATMs for any new Pre-approved Loans messages that appear. Please watch if the Number button wriggle when you use in ATMs. Avoid transactions in that ATMs. Check for Pin hole cameras inserted on top of the Number pad in the ATM. If you find any small object do not transact and report immediately. Do not use passwords from Words in Dictionary. Dictionary attacks have been found successful by hackers. Regularly update your Browser versions and apply security patches. Do not click on messages that request you to update your software especially from Unknown sources. Do not click on software for free trials until due diligence is done.

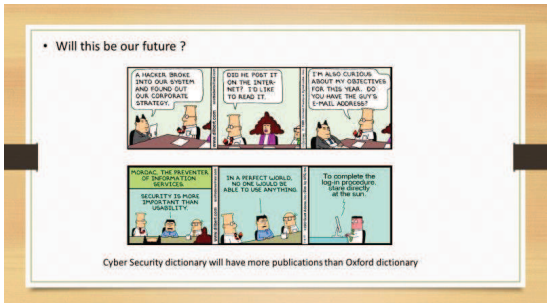
D.2. Shopping Related

Avoid using Debit cards /credit cards in restaurants. If no other option, request the waiter to bring the card machine to your table for swiping. Don't give away the card to the waiter first and expect him to bring the machine. Your card details could have already been stolen. Do not click on any link embedded in email / text message without verifying the authentication. Hackers may post interesting discount offers and request you to click the link. Your mobile and its entire content could be hijacked. Do not store user IDs and passwords in browsers especially the famous shopping websites. Do not store your payment details and if required frequently try changing your CVV with new cards for every six months, if you are a frequent Online shopper. Confirm Online seller's physical address and phone number if case of any questions / problems. Check seller's description of product

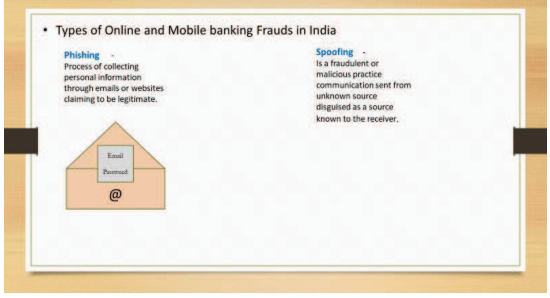
closely. Refurbished, Vintage or Close out indicates product is less than mint condition. Branded items at bargain prices could be counterfeits. Compare same product with multiple shopping sites. Do not send cash or money transfers. Check for Refund policy. Also print or save your online transactions including product description, price, online receipt and related emails. Do not call Customer call helplines from search engine results. Check authenticity of the company's original website and customer support nos. Hijacker may request your bank account details promising refunds but will loot away your bank money. Fraudsters share a QR code over WhatsApp asking for code to be scanned to receive money in their account. You need to scan QR only to make payments not for receiving any payment. Fraudsters ask users to install screen sharing apps such as Screenshare, Anydesk, Team viewer and use them to access bank credentials. These grant access to your mobile data to the third party. Hijackers call offering Cash vouchers on your credit card for Rs.10,000 and request to share verification code he has sent on Victim's mobile no. Once code shared, they start withdrawing money from your account. Online Job frauds and Fake Matrimony sites. You might not be talking to the same person shown in photo / video. These are fake sites and after establishing confidence try to swindle away with your bank money. 47 Online cases in this category registered until last June. Fraud transfer requests from OLX sites have been reported to Cyber Cell. Hijackers claim they have transferred money to your account and request to scan the QR code sent via WhatsApp. Check for the correct brand and serial number of your chosen product. Finish of the product might be different from the website or logo tears off soon. Check brandling locations of the original product and compare with what you received. ContactLess is a chip credit /debit card with the WIFI / wave symbol. This is used in a merchant machine which has also the WIFI symbol. For amount less than Rs.2000 you need not enter PIN. While EMV transactions takes roughly 30 seconds, contact less card takes about 13-15 seconds. If card is stolen, someone else can make contactless purchases. RFID enabled Credit cards – With a pocket size radio frequency scanner cost less than US$ 100 or a high end smartphone with near field communication capabilities (NFC), thieves can obtain data right through your wallet and stand close to you. Wrap Aluminum foil on cards or carry in Aluminium wallet. If your wallet, includes multiple cards with RFID tag in it, the aggregate of data confuses the scanner. Please watch out for people with mobile near your purse especially while standing in the billing section of any merchandise. Use garbage words as passwords in shopping websites, so hackers cannot get any clues. Install Antivirus to detect suspicious websites and files containing malicious programs. Use Adblocker extensions can be installed in browsers Chrome, Firefox etc. Do not click on Advertisements offering money / huge discounts.


Presentation Agenda
Internet Banking – A background
Types of Online and Mobile banking Frauds in India
Cyber Crime Prevention Tips


Internet Usage in India
This statistic provides information on the number of internet users in India from 2015 to 2023. In 2018, India had 483 million internet users. This figure is projected to grow to 666.4 million internet users in 2023. Despite the untapped potential, India already is the second-largest online market worldwide. The majority of India's internet users are mobile phone internet users, who take advantage of cheap alternatives to expensive landline connections that require desktop PCs and infrastructure. As of 2016, India had 320.57 million mobile phone internet users and forecasts estimate
492.68 million Indian mobile phone internet users by 2022.
Number of internet users in India from 2015 to 2023 (in millions)


Will this be our future ?
A HACKER BROKE INTO OUR SYSTEM AND FOUND OUT OUR CORPORATE STRATEGY.
DID HE POST IT ON THE INTERNET? I'D LIKE TO READ IT.
I'M ALSO CURIOUS ABOUT MY OBJECTIVES FOR THIS YEAR. DO YOU HAVE THE GUY'S E-MAIL ADDRESS?
MORDAC, THE PREVENTER OF INFORMATION SERVICES
SECURITY IS MORE IMPORTANT THAN USABILITY.
IN A PERFECT WORLD, NO ONE WOULD BE ABLE TO USE ANYTHING.
To complete the log-in procedure, look directly at the sun.
Cyber Security dictionary will have more publications than Oxford dictionary


Types of Online and Mobile banking Frauds in India
Card skimming -
Theft of credit and debit card data and PIN numbers when the user is at an automated teller machine (ATM) or point of sale (POS). Card skimming allows thieves to steal money from accounts, make purchases and sell card information to third parties for the same purposes.
Skimmer in ATM
Card skimming
Page Jacking -
Process of illegally copying legitimate website content to another website designed to replicate the original website and divert traffic from original site to cloned Web pages.
facebook

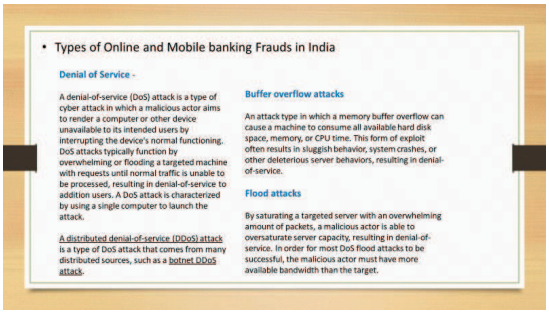

Types of Online and Mobile banking Frauds in India
Phishing -
Process of collecting personal information through emails or websites claiming to be legitimate.
Email
Password
@
Spoofing -
Is a fraudulent or malicious practice communication sent from unknown source disguised as a source known to the receiver.

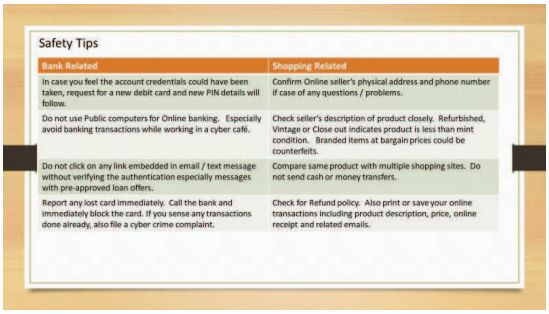

Types of Online and Mobile banking Frauds in India
Juice Jacking -
Juice jacking is a type of cyber attack involving a charging port that doubles as a data connection, typically over USB. This often involves either installing malware or surreptitiously copying sensitive data from a smart phone, tablet, or other computer device.
Beware of Juice Jacking!
Juice Jacking
QR code scam -
A QR code is like a bar code, an image that can be read by a machine. It allows people to make payments by scanning the image and confirming the transaction. Many apps and e-wallets have this feature for easy payment. Most cases QR codes contained malware that drain information from smartphones.
Payment
QR code scam

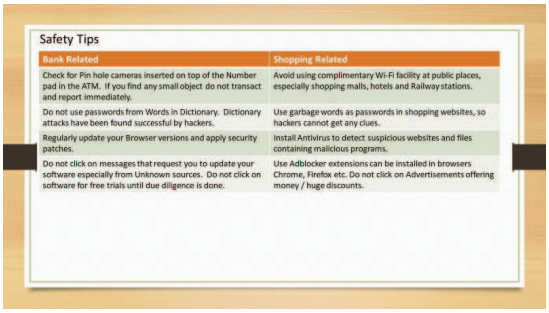

Background
Internet Banking started in the late 1990s. ICICI was the first bank to champion its usage and introduced internet banking to their Customers in 1996. Other banks like HDFC, Citibank and Indusind followed. SBI launched internet banking in 2001.
Anywhere Banking got recognized and services like checking account status, fund transfers, ordering demand drafts, loan applications, shopping portals were viewed as high value offerings.
Total transaction value in the Digital Payments segment amounts to US$64,787m in 2019 from about 513.8 million users in India. The market's largest segment is Digital Commerce with a total transaction value of US$58,812m in 2019. Total transaction value is expected to show an annual growth rate (CAGR 2019-2023) of 20.1% resulting in the total amount of US$134,588m by 2023.
5,743 incidents of fraud involving a total amount of Rs. 95,760 crores from Apr to Sep 2019 reported from Public Sector Banks. Source – Business standard, Nov 20, 2019.

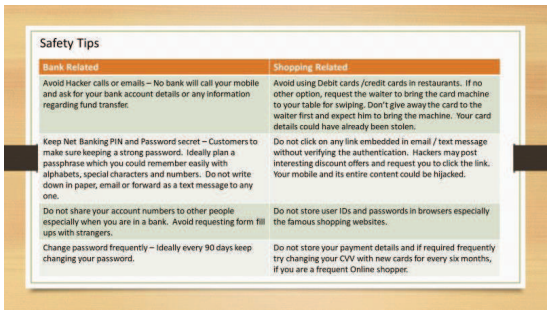

Types of Online and Mobile banking Frauds in India
SIM Swap fraud -
A SIM swap scam (also known as port-out scam, SIM splitting, and simjacking, SIM swapping) is a type of account takeover fraud that generally targets a weakness in two-factor authentication and two-step verification in which the second factor or step is a text message (SMS) or call placed to a mobile telephone. Fraudster contacts the victim's mobile operator and claiming that he has lost the phone. He reaches to the victim to press 1 to approve the SIM swap. Post this the fraudster will start receiving all SMS, OTPs, phone calls and so on.


Cyber Crime Incident Snippets
Central Bank of Bangladesh US$ 100 million stolen
Russian Central Bank US $ 31 million stolen
India's Cosmos Bank loses US$ 13.5 million in Cyber attack
Dutch Bangla Bank lost US $ 3 million
State Bank of Mauritius lost US$ 4 million after recovery of US $ 10 million. Hackers targeted US $ 14 million
https://threatmap.checkpoint.com


Types of Online and Mobile banking Frauds in India
Denial of Service -
A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to addition users. A DoS attack is characterized by using a single computer to launch the attack.
A distributed denial-of-service (DDoS) attack is a type of DoS attack that comes from many distributed sources, such as a botnet DDoS attack.
Buffer overflow attacks
An attack type in which a memory buffer overflow can cause a machine to consume all available hard disk space, memory, or CPU time. This form of exploit often results in sluggish behavior, system crashes, or other deleterious server behaviors, resulting in denial-of-service.
Flood attacks
By saturating a targeted server with an overwhelming amount of packets, a malicious actor is able to oversaturate server capacity, resulting in denial-of-service. In order for most DoS flood attacks to be successful, the malicious actor must have more available bandwidth than the target.







References:

Internet sites